Headquarters U.S. Air Force

Integrity - Service - Excellence

Air Force Cyber S&T Portfolio

Captain Bobby Birrer
SAF/AQR

U.S. AIR FORCE

Distribution A. Approved for public release; distribution is unlimited. SAF/PA Public Release Case No. 2013-0247

U.S. AIR FORCE

Outline

- AFRL Overview
- Guidance/Demand Signals
- Cyber S&T Strategy
- Transitions
- Broad Area Announcements
- Summary

U.S. AIR FORCE

AFRL Mission

It's not just about the science…
…it's about *leadership* in S&T

AFRL Organization

U.S. AIR FORCE

Commander

Maj Gen William McCasland

Executive Director

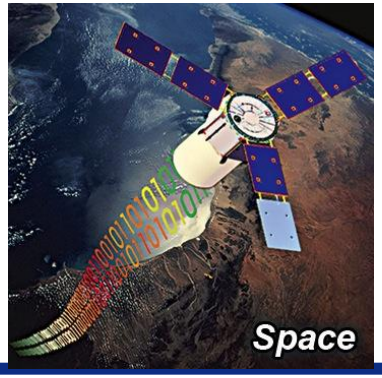
Ricky L. Peters

Vice Commander

Col. Roger M. "RV" Vincent

Chief Technology Officer

Dr. Jennifer Ricklin



Integrity - Service - Excellence

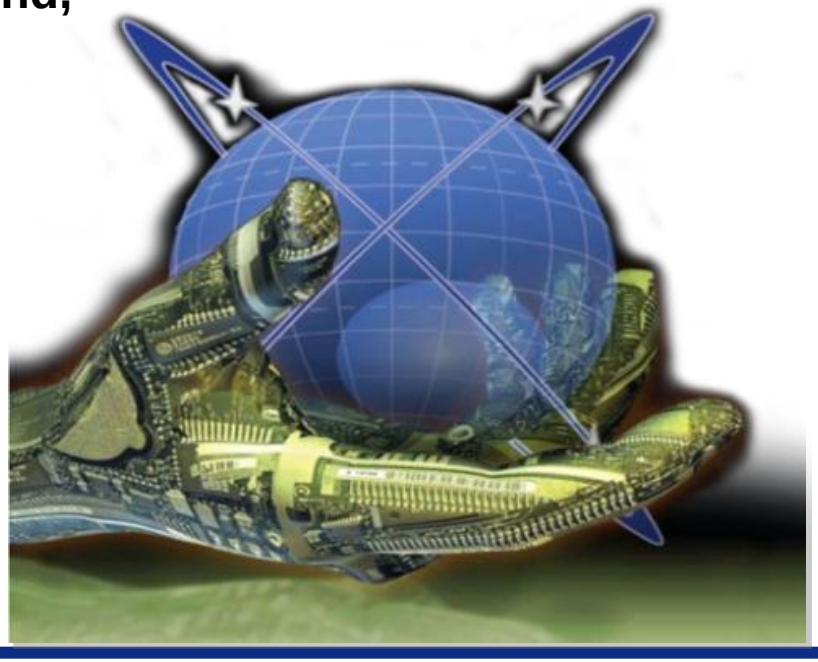
Information Directorate Mission & Vision

Information Directorate Mission

To lead the discovery, development, and integration of affordable warfighting information technologies for our air, space, and cyberspace force

Information Directorate Vision

To defend America by unleashing the power of innovative information science and technology to anticipate, find, fix, track, target, engage, and assess anything, anytime, anywhere.



Information Directorate Core Technical Competencies

RI Programs are organized and planned by CTC

The four core technical competencies provide technologies to translate sensed data to actionable knowledge

Cyber Science and Technology CTC

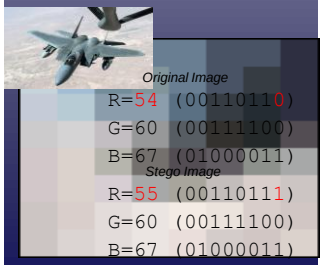
U.S. AIR FORCE

Accomplishments

WiFi Investigator

Advanced Wideband Processor

Steganography



Challenges

- Mission modeling and cyber situational awareness for assuring effective missions
- Cyber agility to disrupt/deny adversary attack planning
- Cyber resiliency to fight through and recover from attack
- Hardware & Software "Root of Trust" for computational platform assurance
- Full spectrum cyber operations for Cyberspace Superiority

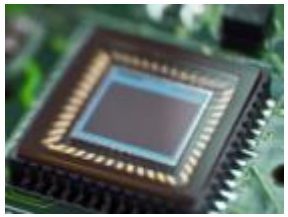
Near (FY12-13)

- Cyber Agility via IP hopping and instruction set morphing at sub-second rates
- Tactical cyber ops able to simultaneously affect multiple nodes (ESC)
- Comm Exploitation capabilities for airborne ISR (Intel Community)

Mid (FY14-17)

- Content/Mission-Aware trusted router 10Gb/sec for 24 AF
- 80% mission aware traffic for 24 AF
- Integrated Information Operations / SIGINT (USCYBERCOM)

Far (FY17-beyond)



- Mathematically provable mission assurance
- Agile infrastructure anticipates & reconfigures in real time
- Integrated/synchronized execution of effects in cyber, air and space

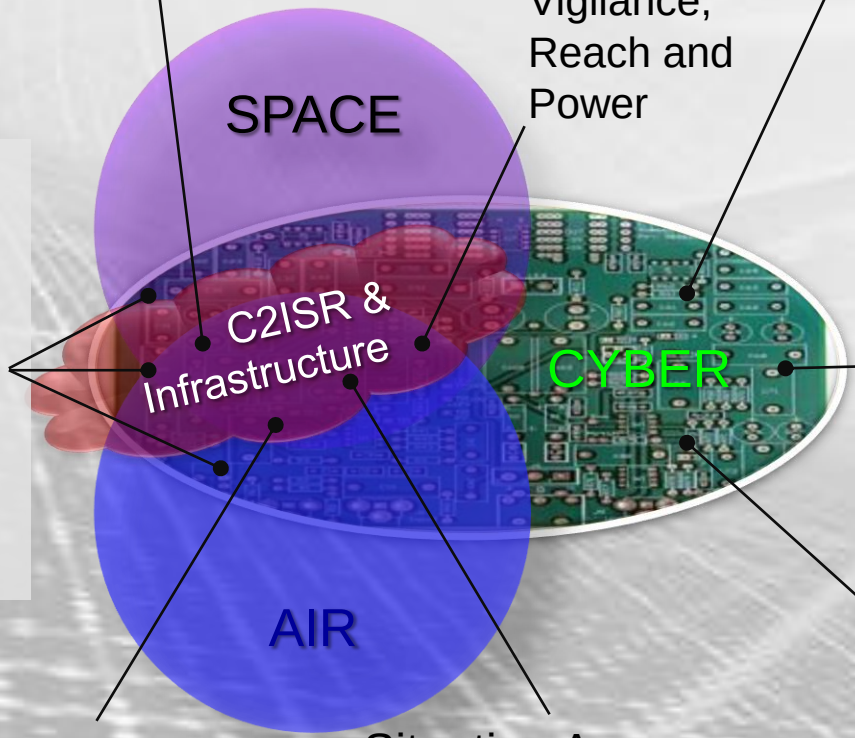
Transition to 24AF, AFSPC, AFLCMC, Intel Community and USCYBERCOM

Operational Environment

Assured Air, Space, C2ISR and Cyber Operations

Global Vigilance, Reach and Power

Networks
Sensors
Data Links
Embedded Systems
Command & Control
Supply Chain
Databases
Operators



Cyberspace = interdependent network of information technology
- Internet
- telecommunications networks
- computer systems
- embedded processors
- controllers
- Individuals
- organizations and missions

Cyber-missions = Cyber exploitation, defense, & operations; information assurance, command & control

Cyber-threats =
- Nation states,
- non-state actors
- domestic threats
- launching/operating agents
- Bots, Trojans, worms
- social engineering
- Insider attacks

Integrated Air, Space, ISR and Cyber Operations

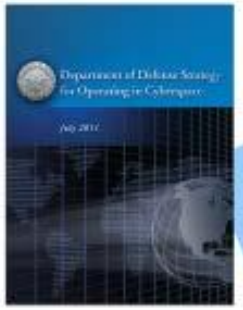
Situation Awareness, Common Operational Picture (COP)

Cyber is Inextricably Entwined with the Air and Space Missions

U.S. AIR FORCE

Strategic Alignment of Cyber Vision 2025

STRATEGY



REQUIREMENTS AND PLANS

COCOM and MAJCOM Requirements

Cyber Vision

United States Air Force
CyberS&T Vision
2011-2025

AF/ST TR 12-01
31 December 2012

Independent Senior Expert Review

MISSION FOCUS

- Threat
- Cyber
- Air Cyber
- Space Cyber
- C2ISR Cyber
- Mission Support (Education & Training, Acquisition, T&E)
- Cross Cutting Enabling S&T

RFIs, EXPERT SUMMITS **CFMPs**

U.S. AIR FORCE

CV2025 Recommendations

- Assure and Empower the Mission
  - Assure national security missions to security standards exceeding business systems
  - More effective use of Title 10/50/32
  - Multi-domain synch/integrated effects
  - Increase cost of adversary offensive cyber operations
- Improve Cyber Education, Accessions, ACE
- Advance processes
  - Require/design in security; secure full life cycle
  - Rapid, open, iterative acquisition; engage user/test early
  - Integrate cyber across Core Function Master Plans
  - Advance partnerships, align funding
- Enhance Systems and Capabilities
  - Reduce complexity, verify systems
  - Hardened, trusted, self-healing networks and info
  - Agile, resilient, disaggregated mission architectures
  - Real-time cyber situational awareness/prediction, managed information objects, cyber FME
- Focused, Enabling S&T
  - Assure and empower missions
  - Enhanced agility & resiliency
  - Optimize human/machine systems
  - Establish foundations of trust

AFRL Cyberspace S&T Strategy

U.S. AIR FORCE

Tenets

ALIGN, LEVERAGE AND GROW

INVENT THE FUTURE

STREAMLINE

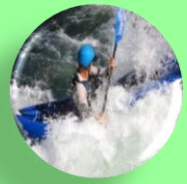
Establish a firm foundation in cyberspace upon which to build mission capability

Assure and Empower the Mission

- Mission Awareness
- Integrated Full Spectrum Operations
- Command, Control (C2) and Decision Support

Enhance Agility and Resilience

- Cyber Maneuver and Response
- Resilient Architectures
- Military-Grade Hardware and Software

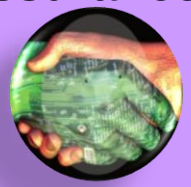


Next-generation AF Cyber Warrior

- Visualization
- Augmentation of the Cyber Warrior
- Cyber Workforce (Select, Educate and Train)

Invent Foundations of Trust and Assurance

- Scientific Foundations of Mission Assurance
- Scientific Foundations of Trust
- Supply Chain Trust



Goal 1: Assure and Empower the Mission

U.S. AIR FORCE

Develop Mission Aware applications and infrastructure that provide integrated full-spectrum cyber capabilities across Air, Space and Cyber

NEAR TERM (2011-2013)

- Cyber Metrics of Performance
- Mission Mapping for selected missions
- Mission Assurance Framework
- Cyber Battle Damage Assessment Tools

MID TERM (2014-2016)

- Real-time mission awareness
- 10Gbit Mission Aware Routing
- Real-time C2 for AFNet
- Cross Service Framework for Information Operations/SIGINT

FAR TERM (2017-2020)

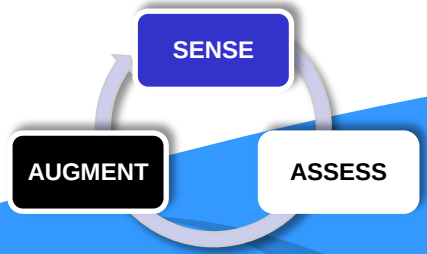
- Map missions in hours
- Assured operations in clouds
- Autonomous execution and reconfiguration in contested environments
- Reconstitute / provision new connectivity
- Self-protecting Information

- **Integrated Full Spectrum Cyberspace Operations**: Develop integrated C2ISR capabilities consisting of offensive, defensive , SIGINT and EW contributing technologies
- **Mission Assurance**: Ensure that the MISSION is a success, not that the “network” stays up; Manage by mission threads with a mission-aware infrastructure
- **Command and Control**: Develop and deliver synchronized C2 operations for and integrated air, space and cyber operating environment

Goal 2: Next Generation Cyber Warriors

U.S. AIR FORCE

Select and train effective cyber-warriors and develop machines & interfaces to enhance human performance with respect to operating in the cyber domain.



NEAR TERM (2011-2013)

- Mission essential competencies
- Objective measures of human trust in automation
- Optimal cyber team composition
- Usability guidelines and metrics

MID TERM (2014-2016)

- Operator mission readiness increased by a factor of two
- Competency based training
- Adaptive interfaces
- Increased situation awareness

FAR TERM (2017-2020)

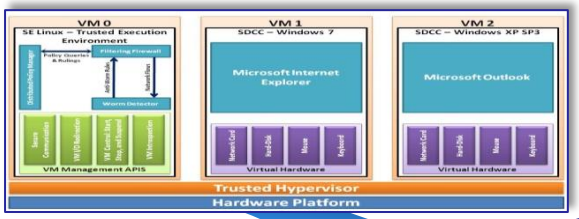
- Update mission view in secs
- Augmented human performance
- Full situation awareness for full spectrum responses
- Measurable metrics of human operator workload

- **Visualization and Common Operating Picture (COP)**: Develop human-machine interface that aids comprehension of cyber events and their relationship to the physical world
- **Cyber Warrior Performance Augmentation**: Combine cybernetics, artificial intelligence and cognitive control technologies to enable operators to be faster and more effective
- **Train the next generation cyber warriors**: Define the necessary aptitude, skill sets, individual characteristics for selection and classification of cyber-warriors; aid the development of training

Goal 3: Enhance Agility and Resilience

U.S. AIR FORCE

Develop techniques for Maneuverability in Cyberspace. Eliminate the adversaries ability to "find" the target. Incorporate Resilience in Cyber systems to enable "fighting through" a contested environment and automatically recovering from an attack.



- Automated/Continuous IP Hopping
- Develop mission enabled cloud computing concepts
- Secure mobile computing platforms
- Hypervisor level protections
- Virtualization capabilities for the AOC

NEAR TERM (2011-2013)

- Threat avoidance metrics
- Instruction set morphing
- Protected root of trust for cyber C2
- Automated protection processes
- Self contained anti-tamper power
- Mission graceful degradation

MID TERM (2014-2016)

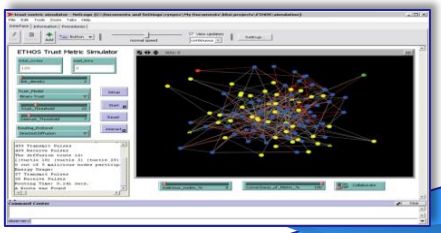
- Predictive assessments
- Agile virtual machine replacement
- Self-healing Networks
- Composable security architectures
- Autonomic anti-tamper

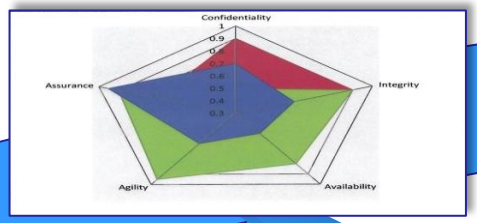
FAR TERM (2017-2020)

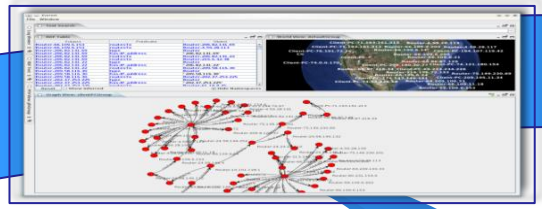
- **Cyber Maneuver and Response**: Develop agile networks that continually change faster than an adversary can find and fix on its target
- **Resilient Architectures**: Develop self-healing network architectures that can degrade gracefully and quickly reboot to reestablish a trusted computing environment
- **Military-Grade Hardware and Software**: Define and develop roots of trust and secure verifiable processes to enable AF-unique systems with trusted components

Goal 4: Invent Foundations of Trust & Assurance

Develop mathematical frameworks for provably correct implementations of trustworthiness and Mission Assurance. Develop trusted hardware, software and data rest/motion techniques that guarantee Confidentiality, Integrity and Authentication.







- Mission mathematical representations
- Secure processor for critical apps
- System decomposition and trustworthiness modeling and metrics
- Reverse engineering and vulnerability analysis tools

NEAR TERM (2011-2013)

- Mathematics for operating in contested cyberspace
- Supply chain assurance techniques
- Automated protection processes
- Destructive/non-destructive microelectronic analysis methods

MID TERM (2014-2016)

- Quantitative risk modeling
- Mathematically provable mission assurance in a contested cyber domain

FAR TERM (2017-2020)

- **Scientific Foundations of Mission Assurance**: Develop a mathematical framework to quantify the security, reliability, and assurance of AF systems
- **Scientific Foundations of Trust**: Develop a framework to analyze cyber systems as they relate to mission essential functions and identify components that require protection
- **Supply Chain Trust**: Develop GOTS equipment for critical systems AND develop technologies, tests, and processes to establish trust with suppliers of COTS equipment

U.S. AIR FORCE

Cyber Technology Recent Success Stories

Secureview

- Securely access multiple security domains from single workstation
- Analysts able to collaborate within a secure community of interest

- Software capability delivered to 13 intelligence agencies under ODNI direction

ODNI

AFISRA

Brasswire

- Provides ability to detect malware on system mother boards

- Software delivered to 688 IOW for test and integration by the 90 IOS

AF Space Command

688 IOW

90 IOS

Image is SRI Inc. TM

Bot Hunter 2.0 for IOP

- Identify and block botnet propagation and C2/Exfil
- Integrated into IOP development platform

- Software capability delivered to enhance Information Operations Platform

AF Space Command

90 IOS

DEU-HBSS Integration

- Data Extraction Utility for Host Based Security System
- Examines zipped and compressed data for malware

- Software module delivered to DISA PEO Mission Assurance

DISA

U.S. AIR FORCE

Broad Area Announcements

- CYBER ASSURANCE TECHNOLOGIES
  - Agility and Resilience
  - Solicitation Number: BAA-11-01-RIKA
- CROSS DOMAIN INNOVATIVE TECHNOLOGIES
  - Trust and Assurance
  - Solicitation Number: BAA-10-09-RIKA
- Cyber Awareness and Resilience Research
  - Assuring Effective Missions
  - Solicitation Number: BAA-RIK-12-03
- INFORMATION INSTITUTE RESEARCH PROGRAM
  - Solicitation Number: BAA-RIK-12-14

U.S. AIR FORCE

Summary

- Cyber S&T strategy derived from demand signals, including *Cyber Vision 2025*, CFMPs, MAJCOMs, and warfighter interactions
- Cyber Portfolio includes activities from basic research through to warfighter transitions
- Air Force Cyber S&T is developing revolutionary and game changing technologies in order to “lead the discovery” in Cyberspace
- S&T mindset focused on delivering capabilities to the warfighter